THE EUROPEAN UNION AND CHINA: TWO DIFFERING APPROACHES TO ETHICS IN ARTIFICIAL INTELLIGENCE

James Lomonosoff

THE AMERICAN POLICY VACUUM

Every day there are more headlines anticipating, with varying degrees of excitement or dread, a world in which artificial intelligence (AI) and machine learning are heavily integrated into our lives. AI has no universally accepted definition, but a European Commission report defines it well enough: AI consists of "systems that display intelligent behaviour by analysing their environment and taking actions–with some degree of autonomy–to achieve specific goals."[1] These range from systems capable of modifying themselves through machine learning (whereby systems rely on data patterns and inferences to perform tasks with limited human intervention)[2] to artificial neural networks (which mimic brain structure to facilitate tasks like image recognition).[3] This future has featured prominently in science-fiction films ranging from *2001: A Space Odyssey* to *Terminator*, as well as in the acclaimed works of authors like Isaac Asimov. It is, perhaps, surprising then that the country which produced Asimov's "Three Laws of Robotics," and which is home to some of the most important centers and businesses developing AI, has yet to develop comprehensive ethical guidelines for the development and use of artificial intelligence. Indeed, President Trump's February 2019 executive order encouraging the development of American AI omits any reference to or variation of the word "ethics."[4] Congress, on the other hand, has yet to pass any legislation specifically addressing limits on AI development.

In the meantime, the other AI superpowers of the world–China and the European Union (EU) –have been far more proactive in attempting to guide the development of AI and define the ethical boundaries within which it can be permitted to function. While their respective policies may appear similar in some regards, they are

[1] *High-Level Expert Group on Artificial Intelligence Working Document on a Definition of AI: Main Capabilities and Disciplines*, at 1 (Apr. 8, 2019), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341.

[2] *Machine Learning*, GOOGLE, https://developers.google.com/machine-learning/glossary (last visited July 16, 2019).

[3] *A Beginner's Guide to Neural Networks and Deep Learning*, SKYMIND: A.I. WIKI, https://skymind.ai/wiki/neural-network (last visited July 16, 2019).

[4] Exec. Order No. 13859, 84 Fed. Reg. 3967 (Feb. 11, 2019).

strikingly different in others. In the absence of an American national policy for AI ethics, it is increasingly the EU and China that are setting the baseline for what can be expected going forward. The goal of this paper is to offer an overview of the EU's and China's ethical guidelines and explore how one can expect them to be applied.

A Brief Introduction to the World of AI Ethics

First, however, it is essential to describe what exactly is meant by AI ethics. The term has broad implications and arises in both the development and use of AI systems. Perhaps the most visceral example of ethics in AI decision-making to have appeared in commentary is the updated version of the "trolley problem."[5] This thought experiment, developed by ethicists and moral philosophers, captures the moral and ethical challenges of binary choices causing life-and-death outcomes. With the growing presence of autonomous vehicles (AVs) on our roads, it has been adapted to cover the scenario of an AV facing an imminent collision having to implement a series of data–processing steps that will ultimately result in assigning higher priority to the lives of certain passengers or pedestrians over those of other involved parties.[6]

Other issues are subtler. For instance, though there may be a tendency to think of AI or machine learning-powered algorithms as neutral arbiters, race or gender bias in the data used by the relevant system may have an impact on its determinations. This was the problem that caused Amazon to cease using a recruiting algorithm it developed to sort through job candidates.[7] In attempting to find candidates whose résumés suggested the potential for success at the company (using the résumés of current employees as a point of

[5] *See* BBC Radio 4, *The Trolley Problem*, YouTube (Nov. 18, 2014), https://www.youtube.com/watch?v=bOpf6KcWYyw (providing an illustrative summary of the problem's various iterations).

[6] Kyle Wiggers, *MIT Study Explores the 'Trolley Problem' and Self-Driving Cars*, VentureBeat (Oct. 24, 2018, 4:40 PM), https://venturebeat.com/2018/10/24/mit-study-explores-the-trolley-problem-and-self-driving-cars/. Further ethical issues have arisen in the context of AI-powered weapons systems capable of taking human life, often called Lethal Autonomous Weapons Systems.

[7] David Meyer, *Amazon Reportedly Killed an AI Recruitment System Because It Wouldn't Stop the Tool from Discriminating Against Women*, Fortune (Oct. 10, 2018), https://fortune.com/2018/10/10/amazon-ai-recruitment-bias-women-sexist/; Alina Tugent, *Exposing the Bias Embedded in Tech*, N.Y. Times (June 17, 2019), https://www.nytimes.com/2019/06/17/business/artificial-intelligence-bias-tech.html.

reference), the algorithm trained itself to penalize applicants who were women (men continue to hold the overwhelming majority of American tech jobs).[8]

Amazon, it seems, was able to determine why its algorithm behaved the way it did; in other cases, it can be practically impossible to establish why a machine learning algorithm came to a specific conclusion. The inability to determine or reverse engineer how or why an AI system produces a certain output is colloquially known as the "black box problem." This occurs when, for instance, an unsupervised machine learning-powered system teaches itself, through trial-and-error, to rely on metrics humans either do not use or do not perceive. Without guidance beyond a coder-given goal (e.g., to maximize profit, in the case of a stock-trading program) and a set of data (e.g., stock market values and trends), a "black box" AI may use unethical ways to carry out its objective (by, for instance, carrying out some form of market manipulation).[9] However, even if something unethical has occurred, the challenge is assessing the "intent" of such a program with regards to its actions.[10] When such an assessment is not possible, "monitoring the 'evilness' of an AI," as one commentator puts it, becomes impossible and laws relying on intent lose their effect.[11] Though human decisions may be affected by subconscious influences, biases, or preconceptions, creating a different sort of "black box" problem, human decision-makers can be held accountable for those decisions in ways AI systems cannot.

Complicating matters further, guidelines that force an AI-powered decision-maker to explain its determinations often do so at the cost of accuracy.[12] Without explainability, so-called "black box" algorithms remain a challenge to those who want to maintain an

[8] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, REUTERS (Oct. 9, 2018, 11:12 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[9] Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, HARV. J.L. & TECH., 890, 906-07 (2018).

[10] *Id.*

[11] Bathaee, *supra* note 9, at 906-07; Théo Szymkowiak, *The Artificial Intelligence Black Box Problem & Ethics*, MEDIUM (Nov. 2, 2017), https://medium.com/mcgill-artificial-intelligence-review/the-artificial-intelligence-black-box-problem-ethics-8689be267859.

[12] *See, e.g.*, Alex John London, *Artificial Intelligence and Black-Box Medical Decisions: Accuracy versus Explainability*, HASTINGS CTR. REP., Jan.-Feb. 2019 at 1, https://onlinelibrary.wiley.com/doi/pdf/10.1002/hast.973.

adequate level of accountability in their products or services. How, for instance, might an algorithm-dependent stock trading company explain to clients why it invested in this or that enterprise if it cannot interpret the calculations of its algorithmic tools? What is the recourse for a customer if those calculations result in a substantial financial loss?

Although Amazon employees and applicants likely consented for their résumé data to be used in that way, the vast amount of personal data that can be used in the creation of an algorithm ensures that consent and privacy, though separate issues, remain intertwined with any discussion of AI ethics. The Cambridge Analytica scandal, which revealed how Facebook had permitted its users' personal data to be used by an outside group to create targeted political messaging without clear consent from its users, is a worthy illustration.[13] With personal information being used in vast quantities to create powerful algorithms, it is little wonder that some see it as the new gold or oil.[14] The extent to which data can be used by companies, to which it can be maintained, to which it can be transferred abroad and to other companies, and to which clear consent must be given for its use will continue to be relevant as political entities approach the formation of comprehensive ethical guidelines.

THE EUROPEAN UNION – HUMANITY-FIRST BUT NO RED LINES

The European Union (EU), perhaps more so than any comparable political unit, has prioritized the rights of individual citizens over state or commercial interests. This attitude, most strongly reflected in the EU Charter of Fundamental Rights,[15] also colors European legislation regarding the rights of private individuals in their personal data. Indeed, the right of "protection of personal data" (Article 8)[16] precedes what, at least in the United States, might be perceived as more fundamental rights like the

[13] Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[14] *The World's Most Valuable Resource is No Longer Oil, but Data,* THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data; *A Personal Data Privacy Model*, COMM. LOGISTICS SPECIALISTS, http://www.communication-logistics.com/personal-data-privacy.html (last visited June 27, 2019).

[15] Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) [hereinafter Charter of Rights].

[16] *Id.* art. 8.

freedoms of thought or expression (Articles 10 and 11)[17]. This is also evident in the more direct regulations of personal data, like the Data Protection Directive[18] and its successor, the General Data Protection Legislation (GDPR).[19]

This has broad implications for the development and use of AI in the EU. Because of the safeguards put in place for private data–the requirement that users unambiguously consent to the collection of data, that they be informed about its use, that they be permitted to have their data modified or deleted, and that the data cannot be transferred to entities or countries lacking these safeguards[20]–the ability of European or foreign entities seeking to use vast datasets is hindered.

Google Spain v. AEPD demonstrated the seriousness with which the EU regards these protections.[21] In that case, which was subject to the Data Protection Directive (having preceded the implementation of the GDPR), Google, as a search engine operator, disputed, amongst other matters, both the fact that the law could be applied when the "processing" of data occurred outside of the EU and that the use of its algorithm to produce search results could even be counted as "data processing" as defined in the Directive.[22] Ultimately, the Court of Justice of the European Union rejected these claims. Paul Nemitz, an official working in the Directorate-General for Justice at the European Commission, characterizes Google's arguments as an attempt "to evade democratic law, and thus responsibility."[23] In this light, the judgment also reflects the

[17] *Id.* arts. 10-11.

[18] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281/31) [hereinafter Data Protection Directive].

[19] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1) [hereinafter GDPR].

[20] *Id.* arts. 32, 39, 101.

[21] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, [2014] C.R., available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN (last accessed July 15, 2019), 2.

[22] Paul Nemitz, *Constitutional Democracy and Technology in the Age of Artificial Intelligence*, PHIL. TRANSACTIONS ROYAL SOC'Y A, Nov. 28, 2018 at 6, https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2018.0089.

[23] *Id.*

EU's concerns about accountability when it comes to the use of personal data in algorithms. Nemitz's suggestion for the future is that respect for the tenets of democracy and rule of law be at the forefront of AI developers' minds as they continue to build systems which utilize personal data.[24]

While the GDPR continues to leave its mark on the development of AI in Europe, the European Commission has since come out with a more focused report from its High-Level Expert Group (HLEG) on Artificial Intelligence: *Ethics Guidelines for Trustworthy AI*.[25] The first acknowledgment the report makes is that AI development and use do not occur in a lawless vacuum – it is already governed in the EU not only by the Union's own laws (e.g., the Charter and the GDPR), but by international treaties as well (e.g., UN Human Rights treaties).[26] Indeed, the report envisions "[a] future where democracy, the rule of law and fundamental rights underpin AI systems."[27] To this end, the HLEG laid out a set of priorities to be considered when determining not what *can* be done with AI, but what *should* be done. These include respect for human dignity, individual freedom, rule of law and respect for democratic institutions, non-discriminatory treatment by AI, and citizens' rights.[28]

The HLEG further reduces these ideas to four overall principles which should apply beyond their present incorporation into law: **respect for human autonomy**, **prevention of harm**, **fairness**, and **explicability**.[29] While the first three are traceable to the longer set of priorities above, explicability ties more directly to the "black box" problem mentioned earlier. Where inputs cannot be adequately explained, the experts write, systems should nevertheless follow other measures–such as clear communication on what a given system can do or is meant to do–to avoid Kafkaesque scenarios in which those affected by algorithmic decisions have no means to contest them.[30]

Nevertheless, the guidelines do not go as far in limiting what AI-operators can do with their work as Nemitz might have suggested.

[24] *Id.* at 13.

[25] *High-Level Expert Group (HLEG) on Artificial Intelligence Report on Ethics Guidelines for Trustworthy AI*, (2019) [hereinafter HLEG on Ethics Guidleines], available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

[26] *Id.* at 8.

[27] *Id.* at 11.

[28] *Id.* at 12-13.

[29] *Id.* at 14.

[30] *Id.* at 15.

Rather than creating conclusive red lines barring certain uses of AI, the guidelines provide a non-exhaustive list of what are labeled as areas of "critical AI concern": AI which tracks individuals, situations where users do not know they are interacting with an AI, AI systems that score individuals (e.g., to assign moral or ethical scores), and lethal autonomous weapons systems.[31] The report notes that many such uses are already illegal under European or national law, but concludes that the ethical ramifications of those activities cannot yet be fully understood.[32] Why, given the priorities of the group, did the experts not create any outright prohibitions? Thomas Metzinger, a philosophy professor who was among those assigned to determine which AI uses should be forbidden, claims that corporate interests–such as those represented in the HLEG by the trade association DigitalEurope–pushed for more watered-down language in the final statement.[33] The problem, he argues, is that without red lines, the boundaries of AI are "up for negotiation," inevitably resulting in the erosion of individual liberties in exchange for some measure of economic gain.[34]

The counterargument is that, given the absence of a competitive homegrown AI industry (the vast majority of major AI developers operate out of China or the U.S.), the HLEG might have been hesitant to place additional burdens on potential growth and saw the existing laws of the EU as sufficient in ensuring that Europe-based companies can produce algorithms made more marketable by their consideration for users' rights.[35] The European Council and European Commission have both released statements pointing to the need to facilitate the growth of a European AI industry through investment and research initiatives.[36] This argument grows stronger

[31] *Id.* at 35-36.
[32] *Id.* at 35.
[33] Tom Simonite, *How Tech Companies are Shaping the Rules Governing* AI, WIRED (May 16, 2019), https://www.wired.com/story/how-tech-companies-shaping-rules-governing-ai/.
[34] *Id.*
[35] Edd Gent, *What's Behind the International Rush to Write an AI Rulebook?*, SINGULARITY HUB (June 11, 2019), https://singularityhub.com/2019/06/11/whats-behind-the-international-rush-to-write-an-ai-rulebook/.
[36] *See* Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, COM(2018) 237 final (Apr. 25, 2018) [hereinafter Communication], https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625; Council of the European Union Press Release, European Coordinated Plan on Artificial

over time as the United States appears content to allow corporations to regulate themselves, despite what appears to be corporate enthusiasm for encouraging and participating in the formation of government regulation.[37]

The HLEG report was the first result of an order from the European Commission[38]; the second result, yet to be delivered, will be a set of policy and investment recommendations.[39] According to Thomas Metzinger, this may present an opportunity to direct investment into research that will produce a stricter set of AI policies without undue industry influence.[40] Whether or not that happens remains to be seen, but the EU has shown its willingness to subject commercial interests to strict regulation in the past, such as with the GDPR.

CHINA – THE TWO FACES OF XI JINPING'S PLAN FOR AI LEADERSHIP

1. *Competing in a Global Market – China's Cybersecurity Laws and the Protection of Personal Data*

The EU is not the sole actor in the emerging field of AI ethics. Though China is approaching the issue cautiously, it is also beginning to make its voice heard. It is, perhaps, well known by this point that China has a stated intention of becoming the world's foremost AI innovation center by 2030.[41] Though the People's Republic has no single officially sanctioned set of AI ethics guidelines, state-sponsored institutions have released two sets, neither as comprehensive as their European counterpart: the Beijing AI Principles[42] and the Governance Principles for the New Generation Artificial Intelligence.[43]

Intelligence (Feb. 18, 2019), https://www.consilium.europa.eu/en/press/press-releases/2019/02/18/european-coordinated-plan-on-artificial-intelligence/pdf.

[37] "In January, Google issued a white paper arguing that although the technology comes with hazards, existing rules and self-regulation will be sufficient 'in the vast majority of instances.'" Simonite, *supra* note 34.

[38] *See* Communication, *supra* note 36.

[39] *See* HLEG on Ethics Guidelines, *supra* note 25, at 6.

[40] Simonite, *supra* note 33.

[41] Jeffrey Ding, *Deciphering China's AI Dream*, FUTURE HUMANITY INST., UNIV. OXFORD 10 (2018).

[42] *Beijing AI Principles*, BEIJING ACAD. ARTIFICIAL INTELLIGENCE (MAY 28, 2019), http://www.baai.ac.cn/blog/beijing-ai-principles (last visited July 17, 2019).

[43] National Governance Committee for the New Generation Artificial Intelligence, *Governance Principles for the New Generation of Artificial Intelligence – Developing Responsible Artificial Intelligence*, CHINA DAILY (June 17, 2019)

The first set, the Beijing AI Principles, was released in 2019 by the Beijing Academy of Artificial Intelligence (BAAI), one of many initiatives funded by the Chinese government as part of the wider effort to become the AI vanguard. The Beijing AI Principles are short – a mere two pages compared to the HLEG report's forty-one – and are perhaps more illustrative in what they do not say rather than what they say. They call for AI research and development to be ethical, and list measures developers may, but are not necessarily legally obliged to, take, such as making systems "as fair as possible" and keeping them transparent and accountable.[44] The statement is scant on what these terms specifically entail, particularly in comparison to the EU statement which features a detailed ethical checklist to which AI creators can refer.[45] Interestingly, the statement calls, albeit in less specific terms, for AI developers and users to acquire informed consent before their products are used by individuals.[46]

In contrast to the EU statement, human rights take a back seat, with notions of protecting the democratic process going, perhaps predictably, unspoken. On human rights, the Beijing AI Principles state that "[h]uman privacy, dignity, freedom, autonomy, and rights should be *sufficiently* respected."[47] (emphasis added). It may be that this is simply an issue with the translation or this may be a deliberate word choice. In any case, what constitutes "sufficient" respect for human rights may be inferred from the rest of the statement, the general tenor of which suggesting that AI's advancement is less for the benefit of the individual and more for society as a whole.

The Governance Principles for the New Generation Artificial Intelligence were released within a month of the Beijing AI Principles by another initiative involved in China's greater AI plan, the National Governance Committee for the New Generation Artificial Intelligence.[48] Also remarkably short, the statement does little to build on that released by BAAI. It calls for respecting human rights but places the need for "social security" (in essence, ensuring a peaceful, law-abiding society) first.[49] Like its BAAI predecessor,

[hereinafter Nat'l Governance Committee], www.chinadaily.com.cn/a/201905/17/WS5d07486ba3103dbf14328ab7.html.

[44] *Beijing AI Principles*, *supra* note 42.

[45] HLEG on Ethics Guidelines, *supra* note 25, at 26-31.

[46] *Beijing AI Principles*, *supra* note 42.

[47] *Id.*

[48] Nat'l Governance Committee, *supra* note 43.

[49] *Id.*

the Committee's piece also stresses the need for AI-users to be informed of potential risks, but, unlike the Beijing AI Principles, does not call for their outright consent.[50]

Generally speaking, these statements on AI ethics appear to be an effort on China's part to get involved in the global ethics conversation before they lose the ability to influence its direction.[51] This would certainly be in line with the Chinese government's desire to set the pace in AI development and seize the "strategic high ground."[52] Professor Chen Xiaoping, who set up the Professional Committee for AI Ethics under the auspices of the Chinese Association for Artificial Intelligence (itself the only state-level group of its type), has said that "the mission of AI ethics should be about maximizing benefits rather than putting restraints on what can be deployed."[53] In this, he echoes the thought process behind the lack of red lines in the EU's ethics guidelines. The reasoning may well be similar: in order to compete with the United States' relatively unhindered tech giants, the government should exercise restraint in barring any potential avenues of success.

One can find more evidence that China is positioning itself to be a major participant in the global AI/data market in the recent legal actions undertaken against Datatang, a company which provides data for use in AI development. Following a lengthy investigation, Shandong Province arrested over fifty individuals connected to Datatang and ten other companies, for infringement of personal information on the scale of "billions of pieces [of data]."[54] The case is, perhaps, less significant in its particulars than it is in indicating a possible trend in Chinese enforcement of data privacy moving forward. Although it was previously understood that wrongful collection or dissemination of private data must become

[50] *Id.*
[51] Gent, *supra* note 35.
[52] Ding, *supra* note 41, at 12.
[53] *China Focus: China Addresses Building Ethical AI*, XINHUA (June 12, 2019), http://www.xinhuanet.com/english/2019-06/12/c_138137273.htm.
[54] Jeffrey Ding, *ChinAI Newsletter #19: Is the Wild East of Big Data Coming to an End? A Turning Point Case in Personal Information Protection*, CHINAI NEWSLETTER (July 16, 2018), https://chinai.substack.com/p/chinai-newsletter-19-is-the-wild-east-of-big-data-coming-to-an-end-a-turning-point-case-in-personal-information-protection; Dr. Yanqing Hong, *Interesting Comments on the Datatang Incident for the DPO (Data Protection Officers) Community*, TSINGHUA UNIV. PRESS (July 10, 2018), https://mp.weixin.qq.com/s/HihJDo1OMrGgVnpFzgUFeA [trans. Jeffrey Ding, https://docs.google.com/document/d/1cZ5vsOsyjQLFKUdQQdtqs1p6C-i00VC2QM2Mkpuj1qI/edit#].

"serious" in scale before constituting an actionable violation, the case clarified that the threshold for legal action is in fact rather low, which would bring Chinese policy closer to conforming with the GDPR (or California's soon-to-be-implemented California Consumer Privacy Act[55]).[56] That said, China's use of vague, non-committal language in many of its regulations may allow the government leeway in whom it chooses to prosecute (it is frequently the case, for instance, that World Trade Organization standards are downgraded to mere recommendations within China to offer similar flexibility).[57] Jeffrey Ding, who has written extensively on Chinese AI policy, suggests that the differences in China's data regulations indicate that the government seeks to advantage Chinese companies over foreign competitors entering the Chinese market through strict control of the outflow of data–an approach some have labeled "techno-nationalism."[58]

As the rest of the AI world, led by the EU, conforms more and more to GDPR-style data regulation, China likely perceives the need to become stricter in enforcing its own, similar policies[59] if it is to adapt to and participate in the expanding market. By continuing AI research and development, including the creation of essential patents (to increase foreign reliance on China's AI industry), the Chinese government will be well positioned to, as Tan Tieniu, Deputy Secretary-General of the Chinese Academy of Sciences, put it, "seize its right to speak in the formulation of international AI standards."[60]

2. *The Security-first Approach of the Chinese Government and the Export of the Surveillance State*

If the normalization of China's AI/data economy is one side of the Chinese approach, then reported human rights abuses at the

[55] *See* Cal. Civ. Code §§ 1798.100-1798.199 (Deering 2019).

[56] Hong, *supra* note 54.

[57] Samm Sacks & Manyi Kathy Li, *How Chinese Cybersecurity Standards Impact Doing Business in China*, CTR. STRATEGIC & INT'L STUD: CSIS BRIEFS, August 2018. at 1, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180802_Chinese_Cybersecurity.pdf?EqyEvuhZiedaLDFDQ.7pG4W1IGb8bUGF.

[58] Ding, *supra* note 41, at 18.

[59] As embodied in the Personal Information Security Specification.

[60] Gregory C. Allen, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*, CTR. NEW AM. SEC, 15 (Feb. 6, 2019), https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Understanding-Chinas-AI-Strategy-Gregory-C.-Allen-FINAL-2.15.19.pdf?mtime=20190215104041.

hands of China's AI-powered security state are the other. While increased enforcement of data protection laws may make China's market and products more palatable abroad and satisfy one common requirement for ethical AI, the Chinese government has pursued policies that belie the other elements of the nation's own ethics statements. These include the increasingly widespread use of AI facial recognition systems in law enforcement, the potential use of AI in supporting China's nascent "social credit" system, and the integration of AI into military systems.

Despite the fact that China's law enforcement practices can be somewhat opaque to outside observers, much has been written in both Chinese and international press about the increasing use of facial recognition AI in apprehending criminal suspects. Its application may still be far from universal, but instances of its use have been touted as heralding a new era in policing.[61] For instance, at an annual beer festival in the port city of Qingdao, facial recognition was used in the identification and subsequent arrest of over twenty criminal suspects who chose to attend.[62] Although the use of facial recognition technology (in both security and advertising contexts) has received its share of criticism in the EU and United States, other, exclusively Chinese uses have been more roundly criticized.[63]

In the western region of Xinjiang, the Chinese government is reported to have been systematically suppressing Uyghurs, a largely Muslim ethnic group that has lived there for centuries.[64] According to the *New York Times*, the state has employed facial recognition algorithms specifically taught to flag Uyghur

[61] Zhou Jiaquan, *Drones, Facial Recognition and a Social Credit System: 10 Ways China Watches its Citizens*, S. CHINA MORNING POST (Aug. 4, 2018), https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china.

[62] Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[63] Holly Richmond, *The Ethics of Facial Recognition Software*, CENT. FOR DIG. ETHICS & POLICY (2013), https://www.digitalethics.org/essays/ethics-facial-recognition-software.

[64] Chris Buckley, *China Is Detaining Muslims in Vast Numbers. The Goal: 'Transformation'*, N.Y. TIMES (Sept. 8, 2018), https://www.nytimes.com/2018/09/08/world/asia/china-uighur-muslim-detention-camp.html?module=inline; Darren Byler, *China's Hi-tech War on Its Muslim Minority*, THE GUARDIAN (Apr. 11, 2019), https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition.

individuals caught on camera (Uyghurs typically have features that are distinguishable from those of the Han Chinese majority), as well as record their comings and goings.[65] Previously thought to be limited to Xinjiang, the scope of this project has reportedly been extended to China's more prominent coastal cities as well as other urban centers, where police have expressed desire to use the systems for "minority identification."[66] If these reports are accurate, these actions would stand in stark contrast to the latest of China's released ethics statements, which calls for "prejudices and discriminations" to be eliminated in product application.[67]

Compare this to China's increased enforcement of data protection policies and it appears there may be two simultaneous yet divergent trends in the growth of AI in China: on the one hand, the curbing of careless data practices suggests that the more internationally accepted rulesets (such as the GDPR) will be respected and incorporated into domestic policy in order to further China's economic interests; on the other, the Chinese government appears to give itself a free hand in using AI technology to further its own "security"-focused agenda. Such a seemingly disparate set of priorities may seem less surprising when one considers that most Chinese statements enumerating citizen rights—whether it is the Personal Information Security Specification[68] or the Constitution[69]— provide that national security supersedes any such rights. As an illustration, in connection with the alleged suppression of the Uyghur population, the *New York Times* reports that the Chinese government has been collecting genetic data without the explicit consent of those whose DNA it is.[70] In one instance, individuals were reportedly offered free medical exams which are

[65] Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

[66] *Id.*

[67] Nat'l Governance Committee, *supra* note 43.

[68] *See* Mingli Shi et al., *Translation: China's Personal Information Security Specification: The Chinese Government's First Major Digital Privacy Rules*, NEW AMERICA (Feb. 8, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/ (last visited July 22, 2019).

[69] *See, e.g.*, XIANFA, art. 28 (1982) (China).

[70] Sui-Lee Wee, *China Uses DNA to Track Its People, With the Help of American Expertise*, N.Y. TIMES (Feb. 21, 2019), https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html.

believed to have been used to collect genetic samples.[71] In another, reporting suggests that genetic data from a Yale professor's own research was used to further complete a Uyghur genetic profile.[72] Such actions would constitute clear violations of personal information protections in China's own laws, but the government justifies them as making the region's people "feel much better and much more happy and secure." [73] In essence, because the government argues there are security concerns at stake, they are permitted to act.[74] From the perspective of a nation that offers citizens more substantial rights against the government, this may seem oppressive or a disproportionate response at best, but to the extent it can be determined from the outside, Chinese citizens largely welcome these law and order developments.[75]

This technology also appears to be coming into play in China's wider foreign policy. Xi Jinping's Belt and Road Initiative constitutes China's bid for economic and political influence over a wide area including much of Asia and Africa through the development of joint infrastructure projects and Chinese investment. Coupled with this effort is the sale of China's surveillance technology and methodology abroad. A recent report by Freedom House[76] indicates that at least eighteen countries are receiving aid from China or Chinese enterprises in building their own monitoring systems.[77] *Nikkei* reporting suggests that many of these countries – Thailand, Myanmar, and Malaysia to name a few – straddle the line between authoritarian and democratic rule and that the export of this technology is thus part of a broader effort to quash or slow any democratic tendencies and bolster support for China in the region.[78] The end result of these divergent approaches to AI ethics is that China can continue encouraging such governments with

[71] *Id.*
[72] *Id.*
[73] Nick Cumming-Bruce, *China's Retort Over Its Mass Detentions: Praise From Russia and Saudi Arabia*, N.Y. TIMES (July 12, 2019), https://www.nytimes.com/2019/07/12/world/asia/china-human-rights-united-nations.html?searchResultPosition=2.
[74] Wee, *supra* note 70.
[75] Mozur, *supra* note 62.
[76] FREEDOM HOUSE, *Freedom in the World 2019* 7 (2019), https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf.
[77] Hiroyuki Akita, *China is Exporting AI-driven Authoritarianism*, NIKKEI ASIAN REV. (June 14, 2019), https://asia.nikkei.com/Spotlight/Comment/China-is-exporting-AI-driven-authoritarianism.
[78] *Id.*

sophisticated AI-powered technology while at the same time bringing commercial uses of AI into compliance with more internationally accepted AI ethical standards.

AI ETHICS – WILL THE U.S. JOIN THE DEBATE?

AI ethics will come to define many of the ways artificial intelligence and machine learning algorithm technology gets developed and used over the coming years. It will power our cars, assess job candidates, aid doctors and lawyers in their work, and more. How countries or international bodies choose to regulate AI will necessarily impact its development, particularly when it comes to multi-national corporations. The EU, first to state its position, takes an altogether cautious approach towards the technology–marking no red lines, but clearly cautioning against what they perceive as harmful outcomes (e.g., AI-powered discrimination or the erosion of human autonomy). China appears to have fewer such scruples in how its government uses AI—as in its systematic documentation and suppression of Uyghurs—but prioritizes ethical AI development in the commercial field as a means to grow its share of the global market and thus achieve its dream of supremacy in the AI field. Although China may be exporting its authoritarian systems to those over whom it seeks to influence, it may also be attempting to bring its corporations in line with the GDPR in order to remain competitive. In that light, and in light of the fact that other regions are on the cusp of adopting similar policies, the EU has more or less set the baseline for ethics in commercial AI today.

The U.S., meanwhile, has continued to go its own way, with AI ethics more or less restricted to the boundaries corporations set for themselves.[79] Where companies have had shortcomings, workers themselves have attempted to pick up the slack.[80] For instance, Jack Poulson, a researcher who resigned in protest from Google, has set up Tech Inquiry, an organization dedicated to making it easier for employees concerned about potential unethical applications to be heard and to increasing transparency regarding

[79] *See, e.g.*, *Artificial Intelligence at Google: Our Principles*, GOOGLE AI https://ai.google/principles/ (last visited July 17, 2019); *Microsoft AI Principles*, MICROSOFT https://www.microsoft.com/en-us/ai/our-approach-to-ai (last visited July 17, 2019).

[80] Kelsey Piper, *Exclusive: Google Cancels AI Ethics Board in Response to Outcry*, VOX (Apr. 4, 2019), https://www.vox.com/future-perfect/2019/4/4/18295933/google-cancels-ai-ethics-board. A Google AI ethics board was shut down after a mere week of operation.

project objectives.[81] This atmosphere of private self-regulation mixed with the growing influence of foreign regulations will change if or when the United States federal government breaks its silence on ethical AI practices. Though the U.S. does not typically opine on the ethics of arising technologies, such guidelines can be read into the laws that pass through Congress. However, while there have been state-level efforts to pass GDPR-inspired data protection laws (such as the already passed California Consumer Privacy Act), Congress itself has been rather slow to act. The most prominent Congressional move thus far has been the proposed Algorithmic Accountability Act of 2019[82], which addresses bias in AI decision-making. Whether such legislation can ever reach the President's desk, given the current political climate, remains to be seen.[83]

[81] Alex Hern, *Google Whistleblower Launches Project to Keep Tech Ethical*, THE GUARDIAN (July 13, 2019), https://www.theguardian.com/world/2019/jul/13/google-whistleblower-launches-project-to-keep-tech-ethical?CMP=Share_iOSApp_Other. Poulson quit his job in response to a Google plan, no longer in the works, to build censorship AI for the Chinese government.

[82] Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019).

[83] Efforts to pass GDPR-style legislation in Congress, though broadly agreed upon as necessary, have floundered over the question of whether to allow a private right of action for data breaches.